(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 178 429 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
06.02.2002 Bulletin 2002/06

(51) Int Cl.7: **G06K 7/12**

(21) Application number: **01202851.0**

(22) Date of filing: **23.09.1994**

(84) Designated Contracting States:
CH DE FR GB IT LI LU

(30) Priority: **27.09.1993 US 127250**

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
94928655.3 / 0 721 717

(71) Applicant: **ANGSTROM TECHNOLOGIES, INC.**
Erlanger, KY 41018 (US)

(72) Inventors:
- **Liang, Louis H.**
  Los Altos, California 94022-7420 (US)
- **Marinello, Daniel A.**
  Burlington, Kentucky 41005 (US)
- **Ryan, William J.**
  Underhill, Vermont 05489 (US)
- **Wray, Donald L.**
  Sunrise, Florida 33323 (US)

(74) Representative:
Luckhurst, Anthony Henry William
MARKS & CLERK, 57-60 Lincoln's Inn Fields
London WC2A 3LS (GB)

Remarks:
This application was filed on 26 - 07 - 2001 as a divisional application to the application mentioned under INID code 62.

(54) Authentication system and method

(57) To authenticate and discriminate among articles, authentic articles are marked with predetermined concentrations of fluorescent substances having known emission wavelengths. The articles are illuminated, predetermined wavelength portions of the emission wavelengths are selected and measured, and then compared to previously characterised responses with respect to variables selected from the list consisting of

i) emission wavelengths,
ii) emission amplitudes,
iii) emission delay times, and
iv) spatial distribution.

A positive authentication result is produced if and only if the measured characteristics agree with the characterised responses.

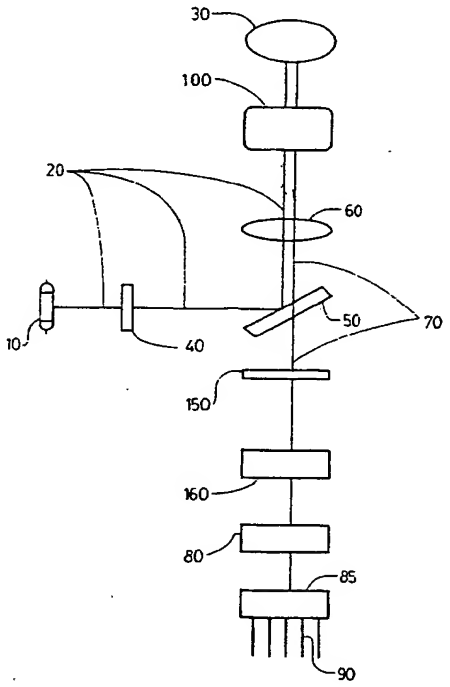

FIG. 1.

EP 1 178 429 A2

Printed by Jouve, 75001 PARIS (FR)

DOCID: <EP___1178429A2_I_>

Description

FIELD AND BACKGROUND OF THE INVENTION

[0001] This invention relates to detection of fluorescent radiation from articles including documents marked with materials that fluoresce when illuminated with non-visible radiation such as ultraviolet radiation. The invention is particularly applicable to detection of counterfeit documents or other counterfeit products and detection of documents or other products which have been subjected to tampering, forging, or other unauthorized modification. Thus the invention is particularly useful for confirming the authenticity and integrity of articles, including valuable documents such as legal papers, identification cards, credit cards, licenses, passports, customs and immigration documents, and valuable mail. The invention can also be applied to quality control of products, providing quantitative and statistical information where the presence or quantity of particular materials is important. Some other examples of applications include label verification, safety seal verification, article alignment, and sorting of articles into two or more categories.

[0002] Many methods have been known in the prior art to authenticate valuable articles. Some known methods include imprinting on the articles a white-light hologram or imprinting reflective and diffractive indicia displaying distinctive images that are difficult to counterfeit. Other known methods include incorporation of distinctive fibers into the articles, such fibers being detectable by visual observation, microwave irradiation, or other means. U.S. Patent No. 4,921,280 describes fibers made luminescent by a dyeing process employing rare-earth compounds, which fibers may be incorporated into articles requiring authentication.

[0003] It is well-known in the prior art that documents may be authenticated by marking the documents with substances such as inks or dyes that appear invisible or relatively unnoticeable to the naked eye in ordinary visible illumination, but that fluoresce when illuminated with ultraviolet light, revealing marks that serve to identify the legitimate document. These methods depend on substances that are not easily or inexpensively identified by a counterfeiter, and not easily or inexpensively duplicated or mimicked by a counterfeiter. When using these methods, it is desirable to use substances such as dyes or inks that fluoresce in narrow spectral bands which are distinguishable by sufficiently narrow-band detectors, but not readily distinguishable by eye. In U. S. Patent No. 4,146,792 by Stenzel et al., these methods are extended to include dyes containing rare-earth elements whose fluorescence is influenced by the chemical environment of the fluorescing atoms in a non-fluorescing matrix, and the detection is refined to include detection of predetermined fine structure in the line spectrum of emitted light. In this method, the spectral fine structure is built into the marking dyes by the formulation of the dyes, and the corresponding discrimination of fine spectral structure is fixed in the physical structure of the checking device by the sizes and positions of photocells cooperating with an optical dispersion element, particularly a narrow-bandwidth interference filter. Yet another class of authentication methods uses substances which fluoresce in the infrared portion of the electromagnetic spectrum when illuminated by light in the visible portion of the spectrum.

[0004] In U.S. Patent No. 4,642,526 by Hopkins and assigned to the assignee of the present invention, a source of ultraviolet light is made self-modulating at a predetermined frequency. Detection of the secondary radiation, filtering of the detected signal, and demodulation of the filtered signal at the predetermined frequency allow the system of Hopkins' invention to detect the fluorescent marks despite interference from ambient light sources.

[0005] Marking products with indicia such as bar codes using fluorescent substances such as inks or dyes is also known in the prior art, both for the purposes described above and for providing identification on the products without detracting from the products' appearance as normally viewed in visible light. U.S. Patent No. 4,983,817 describes methods and apparatus for reading bar codes printed with fluorescent substances, while compensating for variations in background reflectance over the area printed with the bar code.

[0006] In many of the known authentication methods using fluorescence, the fluorescent identifying substance may be incorporated into the article during the article's manufacture instead of marking the article afterwards. One example is incorporating fluorescent substances such as dyes into paper during its manufacture and then using such paper for valuable documents.

[0007] While the various known methods of authenticating articles are useful for many purposes, there is a need for an authentication system that is more readily adaptable by the user, that is reliable, and that provides fast authentication in the presence of optical and electrical noise and bright ambient lighting.

SUMMARY OF THE INVENTION

[0008] An object of this invention is an authentication system that can detect articles marked with fluorescent substances such as inks or dyes to determine whether or not the articles are authentic. A further object of the invention is an authentication system that is adaptable by a user to re-program the discrimination criteria used by the authentication system. A further object is an authentication system that performs reliably in the presence of optical and electrical noise, and is easy to set up, calibrate and verify. Another object is an authentication system with relatively long lamp lifetime. Yet another object is an authentication system that can be manufactured at relatively low cost, and can be made small enough and light enough to be easily portable. A further object is an authentication system that can read bar

codes printed with substances such as inks which fluoresce under ultraviolet illumination, and also read normal visible bar codes, at high speed such as 50,000 scans per minute or more without requiring elaborate schemes for background compensation. A further object of the invention is an authentication system that can acquire and report to its user information, particularly statistical information, about the quality of articles to which it is directed. Other objects are methods of authenticating articles, and methods of encrypting the identity of authentic articles.

[0009] The present invention is based on the use of multi-dimensional and user-programmable discrimination criteria to detect and authenticate indicia on articles. The discrimination criteria may be programmed at the time of manufacture of the articles or later and may be re-programmed by the user at the point of use of the authentication system at any later time. The same authentication systems can be used by many users, with each user having the capability to program discrimination criteria with the complexity and reliability appropriate to that user's needs and appropriate to the value of the articles to be authenticated.

[0010] The various detection criteria used in various combinations by the authentication system of this invention include the wavelengths of fluorescent emission lines, the relative or absolute amplitudes of those emission lines, the time delays of emissions after pulsed illumination with non-visible light, and the spatial distributions of fluorescent materials on the article to be authenticated. The spatial distributions may be bar codes, for example. Or they may be any spatial distributions of marks, such as arrays of dots, characters to be recognized by optical character recognition, images such as half-tone images, signatures, fingerprints, etc.. The combinations of discrimination criteria are used as codes for identifying the authentic article. The indicia made on the articles may include "false" or intentionally misleading codes, i.e. codes that are not actually used as part of the identification criteria combination. For example, bar codes can be printed with fluorescent materials whose emission wavelengths are not tested by the authentication system. If the correct predetermined and programmed combination code is not detected, the authentication system produces a negative authentication result, which may be used to initiate further actions of the apparatus.

[0011] For some applications, the authentication system may optionally include mechanical apparatus to sort authenticated from non-authenticated articles, and may optionally include further apparatus, under some circumstances, to confiscate or destroy unauthenticated articles, e.g. counterfeit credit cards or the like. Alternatively, under some circumstances, the sorted unauthenticated articles may be visibly marked by optional marking means to prevent their continued unauthorized use.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Figure 1 illustrates a schematic diagram of an authentication system according to the present invention. Figure 2 shows a schematic diagram of another embodiment of the authentication system, having a multiplicity of parallel information channels. Figure 3 illustrates a multi-dimensional discrimination space utilized in preferred embodiments of the invention. Figure 4 shows a schematic diagram of a circuit used in the preferred embodiments to provide and interpret signals suitable for detection of predetermined article marking. Figure 5 shows a schematic flow diagram of a method used in a preferred embodiment to detect the predetermined article marking. Figure 6 shows a schematic diagram of an embodiment using a multiplicity of readers.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0013] The authentication system of this invention requires that articles be marked with one or more substances such as dyes or inks which emit light (i.e. fluoresce) in one spectral region, such as the visible region, when illuminated with light in another spectral region, such as the ultraviolet region. Many dye and ink substances which fluoresce are known. Those particular fluorescent substances to be used with the authentication system of this invention are predetermined, and samples of those predetermined substances are used in predetermined concentrations to calibrate and program the authentication system.

[0014] In applications where it is desired to determine if articles have been modified, the fluorescent substances may be erasable. Thus, for example, on a check having erasable fluorescent substances printed in the amount field or signature field, erasure in those fields to modify the check would reduce the amount of fluorescent substance, and that reduction could be detected by a sufficiently sensitive authentication system.

[0015] The authentication system of this invention has a "front-end" portion containing optical elements including a lamp which is a source of ultra-violet light for illuminating an article to be authenticated, a beam splitter, optional scanning means, one or more lenses or mirrors, one or more optical dispersion elements or filters, and one or more photodiodes. The front-end portion is electrically shielded from external electrical noise, where the shielding includes a conductive glass window over the photodiode or photodiodes, with electrical connection between the conductive window and the other shielding. This front-end portion works in cooperation with an electronic portion which provides an AC or pulsed energizing signal for the lamp, processes the electrical signal from the photodiode, provides for calibration of the electrical signal, provides discrimination of the information contained in the signal to authenticate the tested article, and provides various outputs to be described below. The

purposes of these elements and the relationships among them will become clear by reference to the drawings in conjunction with the following more detailed description.

[0016] Figure 1 is a schematic diagram showing the overall functional structure of the authentication system. An ultraviolet light source 10 provides ultraviolet light 20 to illuminate the article 30 to be recognized and authenticated. Article 30 is not part of the invention. If the source's light output contains significant amounts of visible light, an ultraviolet optical filter 40 may be used to block the visible light and to allow the ultraviolet light to pass. The ultraviolet light is directed by a beam splitter 50 toward the article, preferably through a lens 60, which focuses the ultraviolet light upon the article. The lens 60 must transmit both ultraviolet light and the fluorescent secondary light 70 returned from the article. A mirror may be used in place of lens 60. The fluorescent secondary light 70, which is often in the visible part of the optical spectrum, is directed by beam splitter 50 toward a dispersion element or filter set 150 to distinguish selected wavelengths allowed to reach photodetector 160. In a preferred embodiment, element 150 is a simple passband optical filter. The photodetector output is conditioned by electronic signal processing circuits 80, described in more detail below, to produce a signal suitable for analysis by a microcomputer 85. The microcomputer 85 analyzes the signal to produce various authentication result outputs 90, also described in detail below. For applications which require scanning, such as bar code reading, the authentication system also includes scanning means 100. The scanning means 100 may comprise one or more oscillating mirrors or other scanning means known in the art to provide repetitive deflection of an ultraviolet light beam. For some applications, such as the authentication of articles in a production line, the scanning means are not needed in the authentication system, as the articles may be passed before lens 60 automatically, for example by a conveyor belt.

[0017] For some applications, such as authentication of a credit card, it is desirable to have other inputs to the microcomputer, such as a magnetic stripe reader. The information encoded in the magnetic stripe is then used in combination with the fluorescent marking to add yet another dimension to the authentication process. Such combinations of more than one means of authentication can provide better overall security for articles of high value.

[0018] In an authentication system for authenticating articles of high value, portions of figure 1 may be replicated to provide a number of additional parallel channels of information. For example, Figure 2 illustrates a system with three information channels, where the respective analog outputs of the three channels are multiplexed by multiplexer 105. Each channel carries information about a narrow band of fluorescent light from the same articles. For a system as shown in figure 2, the wavelength-selective element 150 is a set of bandpass filters or a dispersive element such as a prism or diffraction grating.

[0019] An important feature of the authentication system is that it uses multiple dimensions of discriminating characteristics to authenticate the markings on articles. Figure 3 shows an illustration of a three-dimensional discrimination space used in the logical operation of the authentication system. Because it is impractical to illustrate discrimination spaces of four or more dimensions by means of a drawing, Figure 3 shows only a simplified scheme in which some of the discrimination dimensions have been omitted for clarity. The three dimensions shown in Figure 3 are (a) the wavelengths 110 emitted by one or more fluorescent materials with which the articles have been marked, (b) the amplitudes of fluorescent response 120 expected from the marks, and (c) the time delay 140 of fluorescent emission expected from the marks. In experiments with apparatus as described here, wavelength differences of less than 50 nanometers and time delays of less than 20 nanoseconds were distinguished. The use of bar codes printed with fluorescent substances, for example, adds a spatial dimension to coding of article marking. The spatial dimension is not limited to bar codes, but may be implemented by using any predetermined pattern distinguished by the localized presence or absence of marks of one or more of the detectable wavelengths of fluorescent emission, or by a predetermined sequence of mark sizes. Such a sequence may be arranged along a particular spatial dimension or arranged in a pattern in more than one spatial dimension. Another manner of using spatial coding uses two or more bar codes printed in the same location on an article and detected by the authentication system as, for example, an invisible bar code printed over a visible bar code.

[0020] A predetermined combination of criteria to be used in authenticating articles may be considered an encryption of the articles' identity. Since that encryption is unknown to potential counterfeiters of the articles, and may be changed by the system user, the encryption provides a high degree of security against counterfeiting.

[0021] Figure 4 shows a schematic diagram of a circuit used in the authentication system to perform the functions of energizing and modulating the ultraviolet lamp 10 at a high frequency, amplifying and synchronously demodulating the weak resulting fluorescent radiation signal from the photodiode 160, and producing an analog output. In one preferred embodiment, the ultraviolet lamp 10 is an ultraviolet cold-cathode fluorescent lamp. It will be understood that the light source 10 of the invention may be any suitable light source. For some applications of the authentication system for example, the preferred light source 10 is a pulsed laser, and suitable modifications are made to the circuit to energize the laser and control its pulse frequency.

[0022] A resonant push-pull inverter circuit 170 (acting as a lamp driver) converts 12 volt DC power to sinusoidal AC at a high frequency of more than about 25

kHz, preferably more than 50 kHz. The frequency is determined by the resonant frequency of an LC circuit made up of a transformer and capacitors in the inverter circuit 170 (not shown). Such inverter circuits are known in the art. In a preferred embodiment, it is desirable to limit the AC current supplied to the lamp 10. The high frequency output of inverter 170 is applied to the ultraviolet lamp 10 to energize it and to modulate its light output at twice the inverter frequency, i.e. more than about 50 kHz, preferably more than 100 kHz. A separate output is tapped from an inductor 180 of the inverter, and the pulses of current at the doubled frequency on this output are filtered and shaped to produce a clock signal for a lock-in amplifier. The inductor 180 may be part of a transformer of the inverter circuit. The current pulses are first filtered with a low-pass filter 190 to produce a substantially sinusoidal wave form, then shaped by slicer circuit 200, such as National Semiconductor voltage comparator circuit LM311, to produce a substantially square wave form. The square-wave signal is adjusted in phase by a first single-shot circuit 210, and adjusted to approximately 50% duty cycle by a second single-shot circuit 220 to produce the desired clock signal 230. In practical application of a preferred embodiment, single-shot circuits 210 and 220 are adjusted to optimize the sensitivity of the authentication system to the authentic articles or their equivalents used as calibration targets.

[0023] The fluorescent light returning from an article to be recognized is detected by a photodiode 160, such as a PIN type of photodiode. The photodiode signal is amplified by two low-noise, wide-bandwidth, high-gain amplifiers 240 and 250, such as Linear Technology LT1028 series ultra-low-noise operational amplifiers. In a preferred embodiment, the total gain of amplifiers 240 and 250 should be about 25,000 or higher. A high-pass filter 255 blocks low frequencies. The amplified and filtered optical signal is synchronously detected by the lock-in amplifier 260. The phase-adjustment single-shot 210 previously mentioned is used to adjust the lock-in clock signal 230 with respect to the phase of the optical signal amplified from the photodiode. The lock-in amplifier 260 comprises an amplifier 270 whose gain is switched between +1 and -1, followed by a low-pass filter 280. The switching of amplifier 270 gain is done by a field-effect transistor (FET) switch 290 driven by the clock signal 230. The low-pass filtered signal goes to a buffer amplifier 300, which produces the buffered analog signal output both to an output connector 310 and to an analog-to-digital (A/D) input 320 of microcomputer 85. The timing of microcomputer 85 operation is determined by a timing element 360, such as a ceramic resonator. Timing element 360 may alternatively be a suitable external clock input.

[0024] Microcomputer 85 may be, for example, a Motorola MC68HC705P9 or equivalent, or any one of a number of microcomputers classified as digital signal processors. In an alternate embodiment of the authentication system, the microcomputer 85 may be timed by a clock generator, and the frequency of lamp driver 170 may be derived from the microcomputer clock signal, as for example by frequency division.

[0025] The analog signal at input 320, produced by the circuit of Figure 4, is converted within digital microcomputer 85 to a digital signal and used by the microcomputer according to its stored program to produce various digital outputs, including outputs to drive a display for displaying information to the operator of the authentication system and other outputs to control sorters or other optional apparatus. In a preferred embodiment, the microcomputer program compares the digital signal with standard digital signals previously stored in a memory portion of the microcomputer. In other embodiments, the microcomputer program and/or the standard digital signal information may be stored in external storage means, such as ROM's EPROM's, memory cards, IC cards, or the like, connected to microcomputer 85 by other connections not shown.

[0026] A number of authentication result outputs are provided by the authentication system for various purposes of users. The simplest output is the analog output of buffer amplifier 300 provided at analog output connector 310. The same signal is applied to A/D input 320 of the microcomputer 85, which processes the signal in a number of ways to produce other outputs. Some additional outputs provided from microcomputer 85 are relay driver outputs 330 and 340 at various voltages, a light-emitting diode (LED) array display 390, and an RS-232 standard serial communication output 350, which also serves as an input port to microcomputer 85. Microcomputer 85 has other inputs, including switch closure inputs 370 and 380 for use by the system operator. Microcomputer 85 may have still other inputs, such as digital inputs from a magnetic stripe reader used in conjunction with the fluorescent marking for further information to be used in determining authenticity of articles.

[0027] Figure 5 is a flow chart illustrating a program used in a preferred embodiment of the invention. In Figure 5, rectangular boxes represent actions and diamond-shaped boxes represent decisions. When the power is turned on (S1), the microcomputer program of the authentication system lights all LED indicators (S2), initializes all internal variables (S3), and calibrates the ambient fluorescent light (S4). The program then begins the main program loop (S5). It reads the calibration switches (S6). If one of them is pressed (S7), the program determines if it is the CALLOW switch (S8). If it is the CAL-LOW switch, the program calibrates and sets the low light limit (S9) and returns. If it is not, the program similarly determines if it is the CAL-HIGH switch (S10). If it is the CAL-HIGH switch, the program calibrates and sets the high light limit (S11) and returns. In an alternative embodiment not shown in figure 5, factory calibration results may be stored in a read-only-memory associated with the microcomputer, and the factory calibrations are then used in later steps of the program, unless

the user over-rides the factory calibration. If no calibration switch is pressed, the program reads the analog signal a predetermined number of times and averages the results (S12). (In other embodiments not shown in figure 5, step (S12) may be triggered by external command, and the function of step (S12) may include other treatments of the signal, other than averaging.) In the sequence shown in figure 5, the program displays the result in an array of amber LED's (S13). It compares the average result with the ambient light calibration (S14). If the result is less than or equal to the ambient, the program turns off both a red LED and a green LED (S15) and turns off both a first and a second relay (S16). The program then compares the average result with the low limit (S17), and compares the average result with the high limit (S18). If the result is less than the low limit or greater than the high limit, the program lights the red LED and turns off the green LED (S19), and also turns off a first relay and turns on a second relay (S20), and returns to restart the main loop (S5). If the result is not less than the low limit and not greater than the high limit, the program turns the green LED on and the red LED off (S21), and also turns on the first relay and turns off the second relay (S22), and returns to the main loop (S5). In this simple and inexpensive embodiment, the user can determine the authentication result by observing the LED's.

[0028] It will be understood that a similar program flow may be used for each of the several discrimination criteria or dimensions employed for discriminating articles by the methods and apparatus of the present authentication system.

[0029] Figure 6 illustrates another embodiment of the invention, which uses a multiplicity of readers to authenticate articles. Indicia of various kinds can be provided on articles known to be authentic. For example, a single article, such as a credit card, could carry ordinary visible bar codes, bar codes printed in fluorescent inks, and codes recorded in a magnetic stripe. In figure 6, article 30 has two kinds of indicia in a predefined field 31 and one kind of indicia in another predefined field 32. A reader 400 and a different reader 410 can both scan field 31 and read the two different kinds of indicia in that field, while a third reader 420 can scan field 32 and read the indicia in that field. For example, reader 400 may incorporate the apparatus described above for reading bar codes printed with fluorescent substances, and reader 410 can be a similar reader adapted for visible-ink bar codes, while reader 420 may be a magnetic stripe reader. The results of the three readers in this example are combined by microcomputer 85 to determine if the article is authentic. Optionally, a multiplexer (not shown) can be interposed between the multiplicity of readers and the microcomputer. It will be apparent that the number of different indicia may be two, or may be more than the three illustrated in figure 6. The security of the authentication scheme is enhanced by using multiple codes. The multiple codes can be combined in various ways unknown to a potential counterfeiter or unauthorized user of the article in question. For example one of the kinds of indicia may carry a key code which is used to allow access to information stored in a removable form of memory used with the authentication system. The access permission would operate similarly to the use of a password in allowing access to an information-processing system or to a particular account on such a system.

[0030] Security documents, such as bank checks, credit cards, driver's licenses, identification cards, legal documents such as wills and contracts may be made to take advantage of the methods of authentication described here. The methods using multiple discrimination criteria can be applied if the security document has two or more fields, at least one which bears indicia made with a fluorescent substance.

[0031] The authentication system is easy to use. The user directs the authentication system's optical front-end portion so that it illuminates the articles to be authenticated or moves such articles past the system's optical front end at a suitable speed and suitable distance, taking into account the focal length and depth of focus of the system's lens. The various authentication result outputs described above indicate whether or not an authentic article has been detected. If an authentication result output has been arranged to sort articles, then the articles are automatically sorted. If optional means to confiscate, destroy, or mark the unauthenticated articles have been included in the authentication system, those actions provided are carried out automatically unless additional means are included to require human confirmation of such actions.

[0032] Another way to use the authentication system is to incorporate the predetermined fluorescent substance such as dye or ink (at a predetermined concentration) into other material that is to be recognized and measured on articles during their manufacture, for quality control. The articles are passed before the authentication system to perform a quality control inspection. The authentication outputs are then recorded by the system microcomputer and analyzed statistically to provide statistical process control or quality control information about the articles. In particular, the microcomputer can be programmed to calculate statistical process control limits and to test each article for conformance to those process control limits. This kind of application of the authentication system is especially useful for monitoring expensive materials. In experiments on controlling a process of applying a non-fluorescent substance to a fluorescent paper, another fluorescent substance was added to the applied non-fluorescent substance at a level of only 0.02% and measured by the apparatus of this invention in the presence of the fluorescent background from the paper.

[0033] In a particularly simple manner of using the invention in one of its preferred embodiments, the operator first turns on the authentication system power, with

no target article present within the view of the system. The system is programmed to read the ambient fluorescent light signal level automatically. The system may be calibrated by presenting sample targets known to produce low-limit and high-limit fluorescent light signals, while pressing the LOW and HIGH calibration limit switches respectively. Thereafter, the system automatically and repeatedly samples the fluorescent light from articles, indicating the result through an array of amber LED's, a red LED, a green LED, and two relays. The array of amber LED's is programmed to show the signal level on a linear or logarithmic scale. If the signal is in the range between the LOW and HIGH limits, a green LED is turned ON, a red LED is turned OFF, and one relay is set to indicate a positive authentication. If the reading is between the ambient level and the LOW limit, or is above the HIGH limit, then a red LED is turned ON, the green LED is turned OFF, and another relay is set to indicate negative authentication. If the reading is at or below the ambient level, both LED's and both relays are set OFF, indicating that no authentication result is available.

[0034] It will be appreciated from the foregoing descriptions of the invention that many other combinations of discrimination criteria may be programmed into the authentication system described.

Claims

1. A method for discriminating among articles marked with one or more predetermined fluorescent substances which emit fluorescent light in response to electromagnetic radiation, comprising the steps of

   a) preparing articles known to be authentic by marking said authentic articles with predetermined concentrations of said predetermined fluorescent substances having known emission wavelengths of said fluorescent light,
   b) characterising the fluorescent responses of said articles known to be authentic with respect to variables selected from the list consisting of

      i) emission wavelengths of fluorescent light,
      ii) emission amplitudes of said fluorescent light,
      iii) emission delay times of said fluorescent light, and
      iv) spatial distribution of said fluorescent light;

   c) illuminating said articles with said electromagnetic radiation,
   d) selecting predetermined wavelength portions of said fluorescent light corresponding to said known emission wavelengths,
   e) comparing the characteristics of said predetermined wavelength portions with said characterised responses, and
   f) producing a positive authentication result if and only if said characteristics agree with said characterised responses.

2. A method of encrypting the identity of articles using one or more substances which emit fluorescent light when illuminated, comprising the steps of

   a) preparing a set of discrimination criteria by

      i) selecting predetermined acceptance limits for the emission wavelength of at least one specific emission line of said fluorescent light as a first characteristic, and
      ii) selecting predetermined acceptance limits of at least one additional

   characteristic of said fluorescent radiation selected from the list consisting of
   emission amplitudes of said fluorescent light,
   emission delay times of said fluorescent light after illumination, and
   spatial distribution of said substances on said articles;
   b) marking said articles with said substances according to said selected characteristics to produce said discrimination criteria when illuminated; and
   c) optionally marking said articles according to other criteria of characteristics not so selected, thereby masking said selected discrimination criteria,

   whereby said articles bear encrypted identity marks.

3. A method of authenticating articles of unknown authenticity, comprising the steps of

   a) encrypting the identity of articles known to be authentic according to the method of claim 2,
   b) illuminating said articles of unknown authenticity with electromagnetic radiation suitable for exciting said fluorescent light,
   c) testing said fluorescent light characteristics with respect to said predetermined acceptance limits of said first characteristic and of said selected additional characteristics, and
   d) producing a positive output if and only if said predetermined acceptance limits are satisfied, thus authenticating only those articles known to be authentic.

4. A security document that can be reliably authenti-

cated, comprising two or more selected fields bearing indicia, at least one of said fields bearing indicia marked with a fluorescent substance, and at least one of said fields bearing indicia made by non-fluorescent means.

5. An authentication system, comprising

a) a first reader means adapted to read first indicia printed with a substance that fluoresces when illuminated with ultraviolet light, having a first output,
b) a second reader means adapted to read second indicia, having a second output, and
c) microcomputer means programmed to receive said first and second outputs respectively from said first and second reader means, to decode said first and second indicia, and to produce an authentication result depending on whether or not said indicia agree with predetermined indicia codes.

6. An authentication system as in claim 5 wherein said second indicia are printed with substances visible in white light, and said second reader means is adapted to read such second indicia.

7. An authentication system as in claim 5 wherein said second indicia are recorded magnetically in a magnetic stripe, and said second reader means is adapted to read such second indicia.

8. An authentication system as in claim 5 wherein said second indicia are recorded in a hologram, and said second reader means is adapted to read such second indicia.

9. An authentication system as in claim 5 wherein both said first and second indicia comprise bar codes.

10. An authentication system for discriminating among articles marked with one or more fluorescent substances which emit fluorescent light in response to electromagnetic radiation, comprising

a) a source of electromagnetic radiation in at least one of the ultraviolet, visible and infrared spectral ranges,
b) means for modulating said electromagnetic radiation at a frequency of more than about 50 kHz,
c) means for synchronously detecting said fluorescent light at said modulation frequency to produce an analog signal,
d) conversion means to convert said analog signal to a first digital signal,
e) comparison means comparing said first digital signal with a predetermined second digital signal to within a predetermined tolerance, and
f) output means indicating a positive authentication result if said first and second digital signals agree to within said tolerance, and otherwise indicating a negative authentication result.

11. An authentication system for discriminating among articles marked with one or more fluorescent substances which emit fluorescent light in response to electromagnetic radiation, comprising

a) a source of electromagnetic radiation in at least one of the ultraviolet, visible, and infrared spectral ranges,
b) a driver circuit adapted to energize said source at a predetermined frequency, and to provide a first clock signal at a frequency selected from said predetermined frequency and a frequency equal to twice said predetermined frequency,
c) a beam splitter disposed to direct said electromagnetic radiation toward said articles and to direct said fluorescent light emitted by said articles toward at least one detector capable of producing a first analog signal responsive to said fluorescent light,
d) at least one optical element disposed to focus said electromagnetic radiation on said articles and to pass said fluorescent light from said articles,
e) at least one wavelength-selective means disposed to allow selected portions of said spectral ranges to illuminate said detector,
f) amplifier means disposed to synchronously detect said first analog signal at the frequency of said clock signal,
g) low-pass filter means removing high frequencies from said detected first analog signal to produce a second analog signal
h) an analog-to-digital converter converting said second analog signal to a digital signal,
i) microcomputer means operating under a predetermined program and comparing said digital signal to one or more predetermined digital signals adapted to discriminate between said marked articles and other articles not so marked, and
j) digital output means indicating authentication or lack of authentication of said articles to be discriminated.

12. An authentication system as in claim 11 wherein

a) said source of electromagnetic radiation comprises a cold cathode fluorescent lamp,
b) said driver circuit comprises a DC to AC inverter having at least one inductive circuit element, and

c) said first clock signal is derived from a tap on said inductive circuit element.

13. An authentication system as in claim 11 wherein said clock signal has a frequency of more than about 50 kHz.

14. An authentication system as in claim 11 wherein said first analog signal is derived from the output of a photodiode responsive to said fluorescent light, said photodiode output is filtered by a high-pass filter to produce a first filtered signal, and said first filtered signal is amplified by at least one amplifier having a total gain of more than about 25,000 to produce said first analog signal.

15. An authentication system as in claim 11 wherein said source of electromagnetic radiation comprises a laser, said driver circuit comprises a pulse generator whose output pulses drive said laser, said predetermined frequency is the frequency of said pulses, and the frequency of said first clock signal is the frequency of said pulses.

16. An authentication system as in claim 11 wherein said optical element comprises optical deflection means disposed to scan said electromagnetic radiation across a portion of each of said articles to be authenticated.

17. An authentication system as in claim 11 wherein said optical element comprises a lens.

18. An authentication system as in claim 11 wherein said optical element comprises a mirror.

19. An authentication system as in claim 11 wherein said deflection means comprises an oscillating mirror.

20. An authentication system as in claim 10 wherein said predetermined second digital signals comprise predetermined bar code signals.

21. An authentication system as in claim 11 wherein said predetermined digital signals comprise predetermined bar code signals.

22. An authentication system as in claim 11 wherein said predetermined program is stored in memory means removable from said authentication system.

23. An authentication system as in claim 11, further comprising sorting means disposed to separate said articles to be discriminated into two or more sets of articles according to said digital output means.

24. An authentication system as in claim 23, further comprising marking means disposed to visibly mark articles discriminated as not authenticated, to prevent their further unauthorized use.

25. An authentication system as in claim 23, further comprising means to hold articles discriminated as not authenticated, to prevent their further unauthorized use.

26. A method for discriminating among articles marked with one or more predetermined fluorescent substances which emit fluorescent light in response to electromagnetic radiation, comprising the steps of

a) preparing samples of said articles known to be authentic by marking with predetermined concentrations of said predetermined fluorescent substances,
b) illuminating said known authentic articles with electromagnetic radiation in at least one of the ultraviolet, visible, and infrared spectral ranges,
c) modulating said radiation with at least one predetermined modulation frequency and at least one first phase,
d) selecting predetermined wavelength portions of said fluorescent light,
e) synchronously detecting said predetermined wavelength portions of said fluorescent light at at least one said predetermined frequency and at a predetermined second phase and a predetermined duty cycle, to produce a first analog signal,
f) filtering said first analog signal with a low-pass filter to produce a second analog signal,
g) adjusting said predetermined second phase with respect to said first phase,
h) adjusting said predetermined duty cycle,
i) measuring the amplitude of said second analog signal,
j) repeating steps (g), (h), and (i) until said second analog signal amplitude is maximized,
k) repeating steps (b) through (f) for articles to be discriminated,
l) converting said second analog signal to a digital signal,
m) comparing said digital signal to at least one predetermined standard digital signal,
n) activating predetermined outputs indicating authentication or lack of authentication of said articles to be discriminated.

27. A method as in claim 26 wherein the step (m) of comparing said digital signal to at least one predetermined standard digital signal further comprises the substeps of

a) comparing the amplitude of said digital signal at a first predetermined time to the amplitude of at least one first said predetermined digital signal,
b) storing the result of said comparison in a first memory location,
c) repeating substeps (a) and (b) a predetermined number of additional predetermined times and storing said results in additional memory locations, and
d) comparing the contents of said first and second additional memory locations with a predetermined pattern.

28. A method as in claim 27 wherein said step (d) of comparing the contents of said memory locations further comprises the substeps of

a) averaging the contents of said memory locations to form an average value, and
b) comparing said average value with predetermined values.

29. A method as in claim 26 wherein said said predetermined standard digital signal is a bar code signal.

30. A method as in claim 26 wherein said steps (b) and (c) are performed with a laser.

31. A method as in claim 26 wherein said predetermined modulation frequency is more than about 1 MHz.

32. An authentication system as in claim 11, further comprising a magnetic stripe reader having a digital output, wherein said magnetic stripe reader digital output is connected to said microcomputer to provide information used by said predetermined program to produce said digital outputs indicating authentication or lack of authentication.

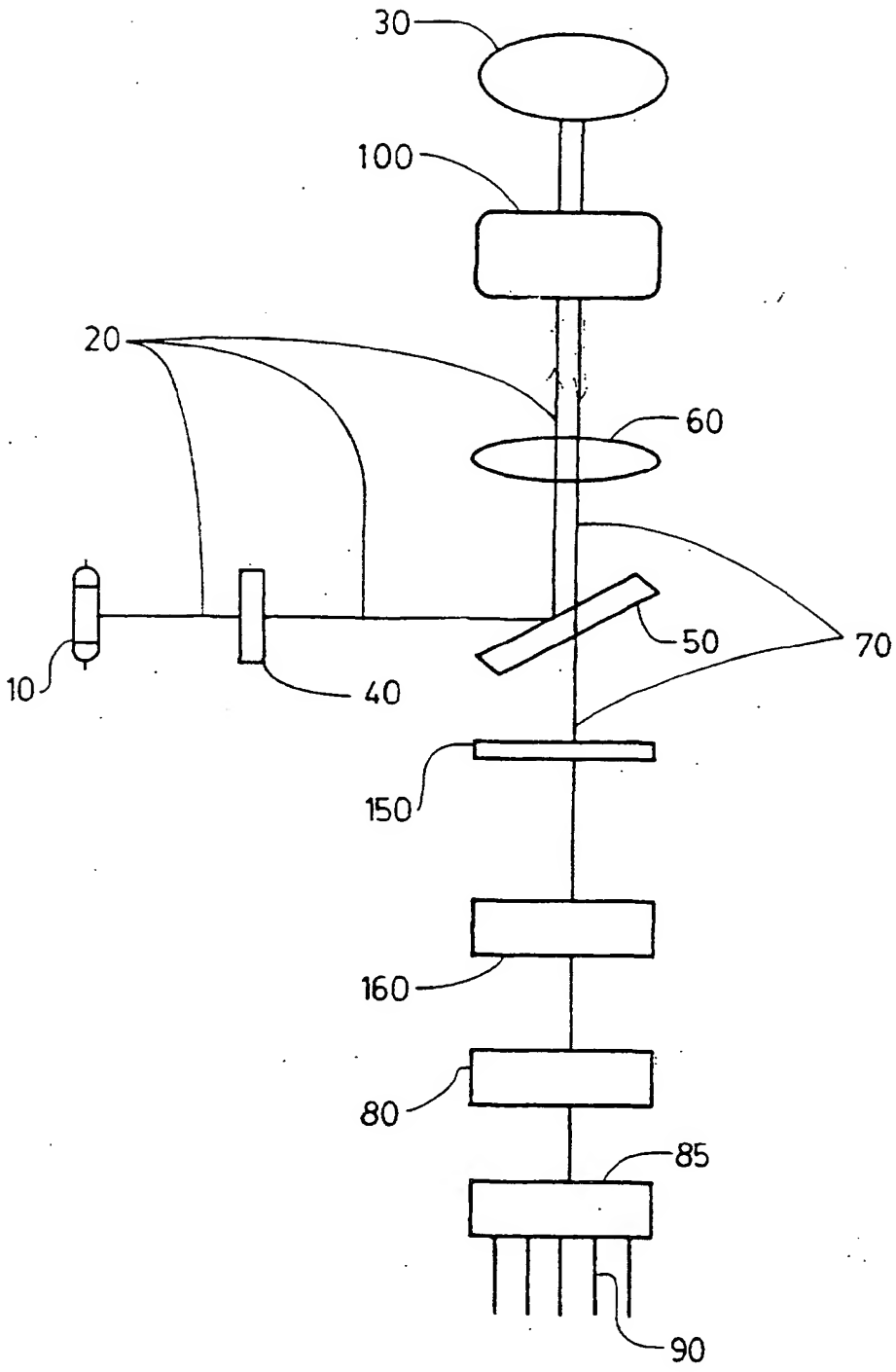

FIG. 1.

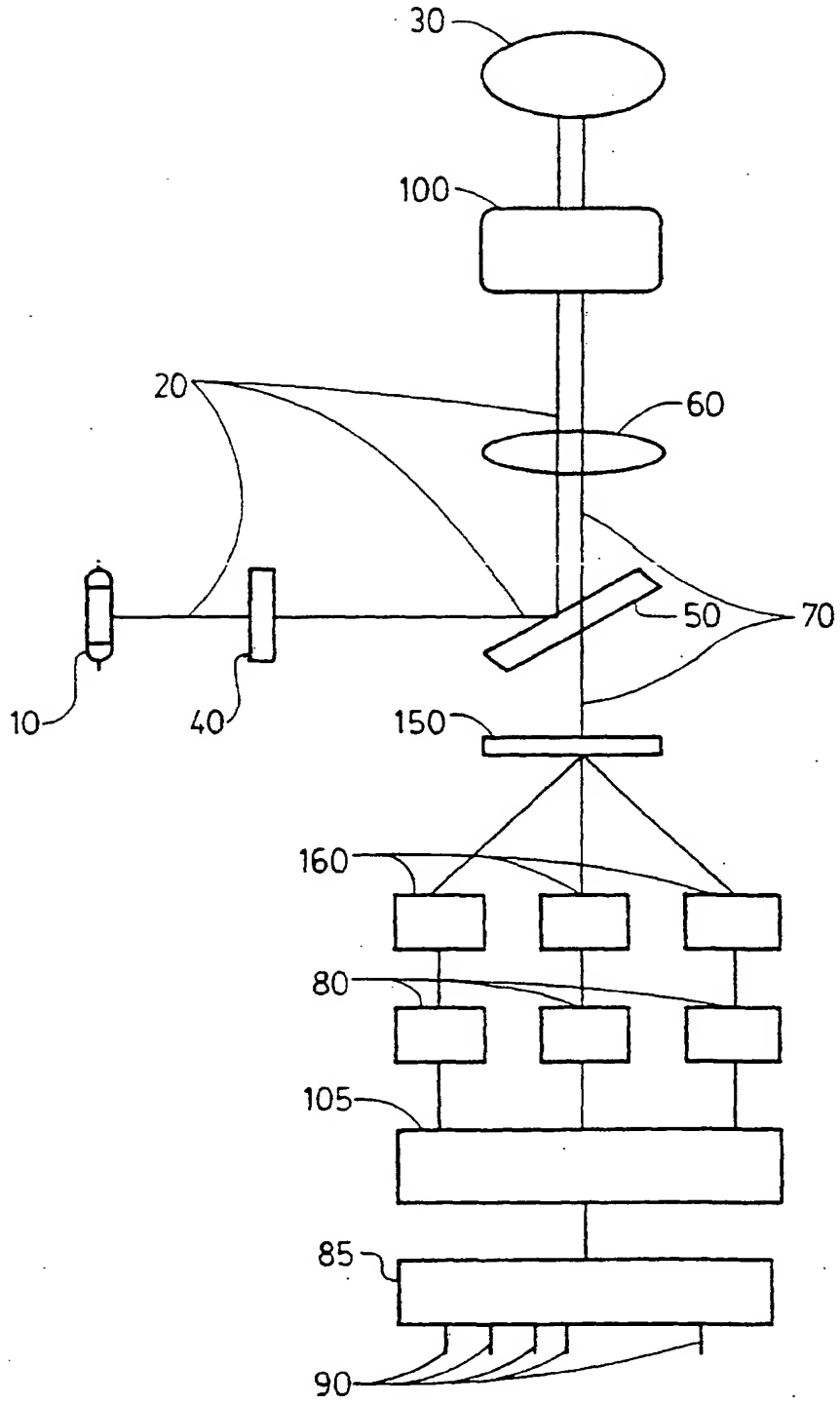

FIG. 2.

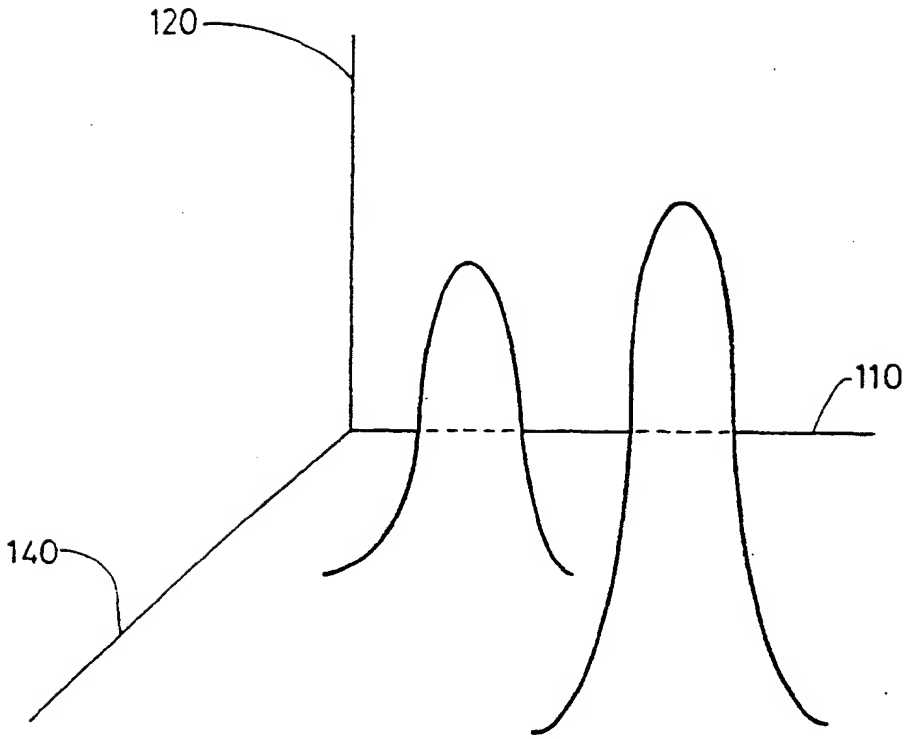

FIG. 3.

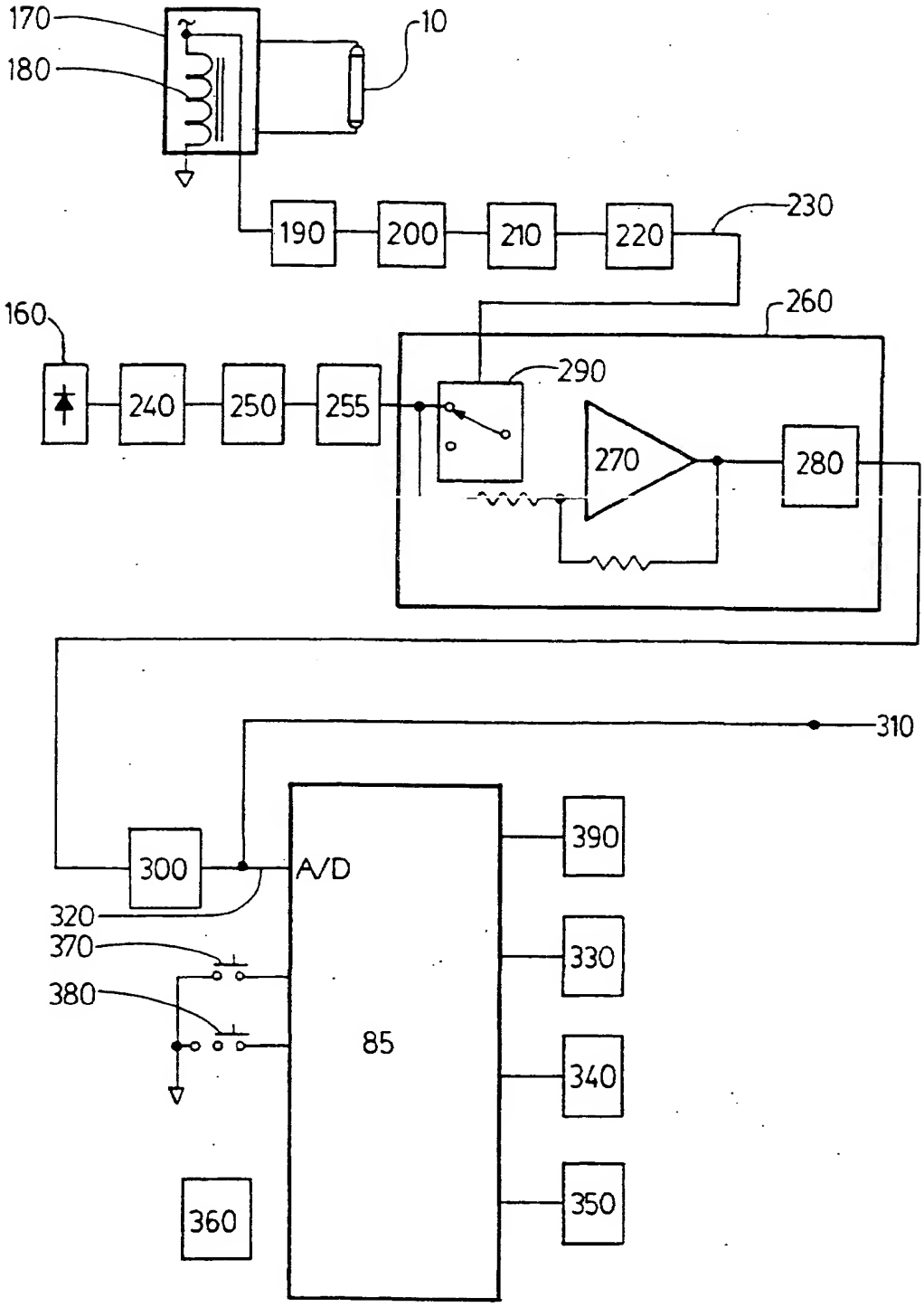

FIG. 4.

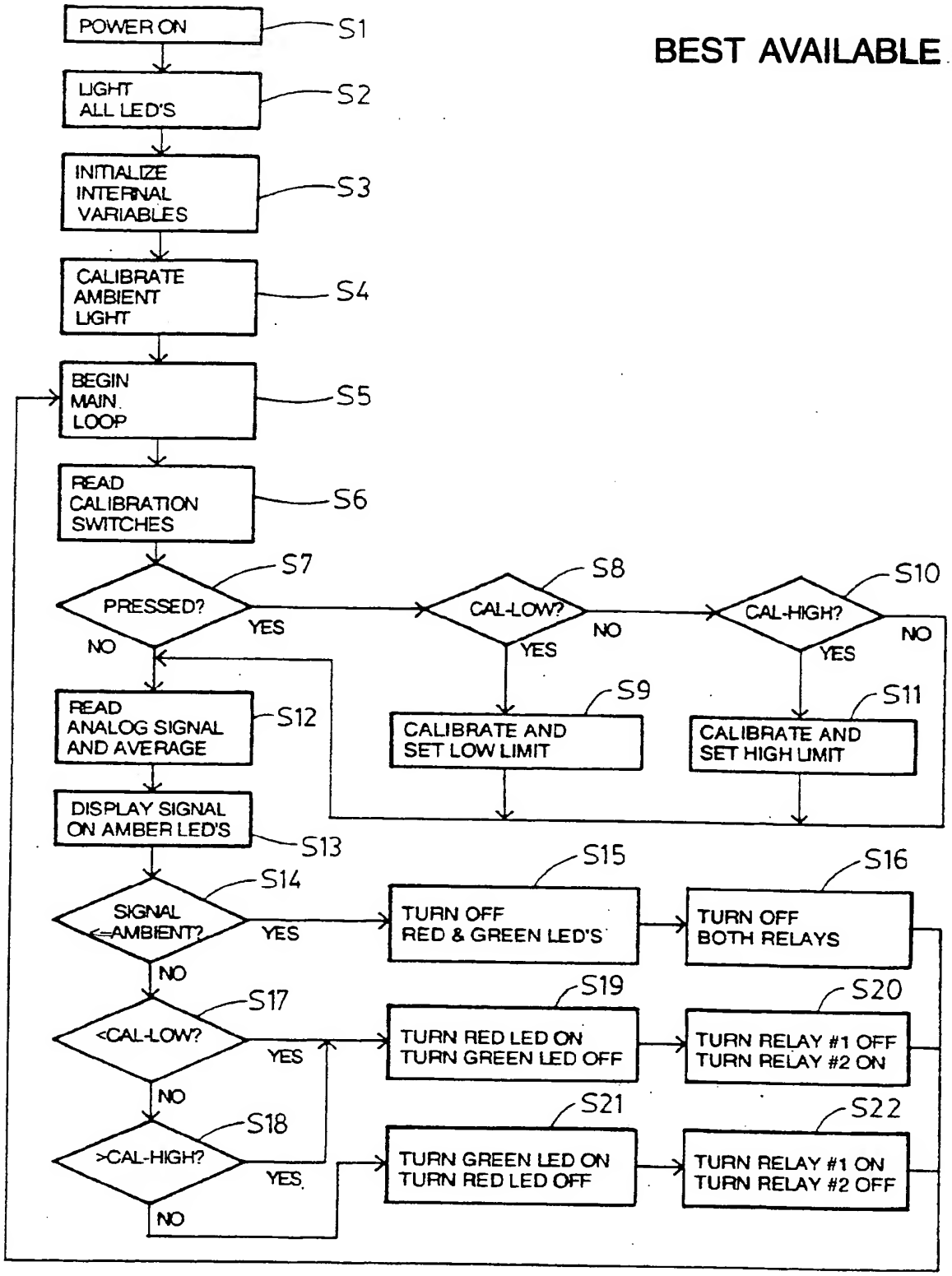

FIG._5.

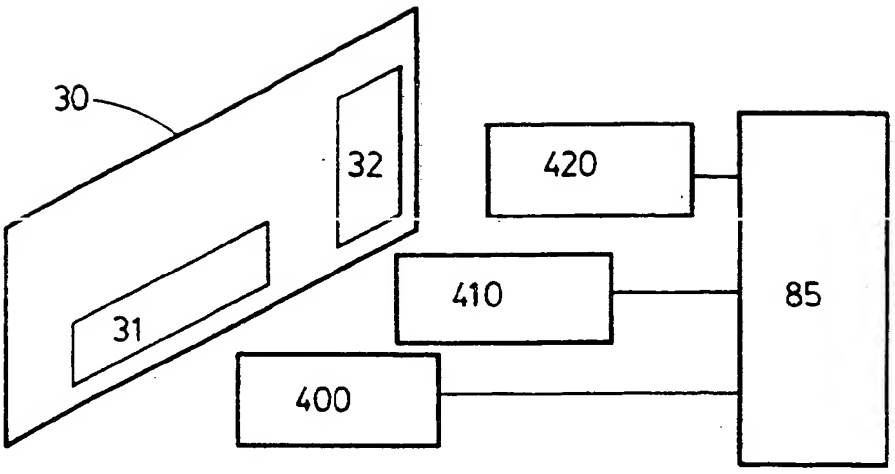

FIG. 6.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 178 429 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
04.09.2002 Bulletin 2002/36

(43) Date of publication A2:
06.02.2002 Bulletin 2002/06

(21) Application number: **01202851.0**

(22) Date of filing: **23.09.1994**

(51) Int Cl.7: **G06K 7/12**, G06K 19/10, G06K 19/14, H04L 9/00

(84) Designated Contracting States:
CH DE FR GB IT LI LU

(30) Priority: **27.09.1993 US 127250**

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
94928655.3 / 0 721 717

(71) Applicant: **ANGSTROM TECHNOLOGIES, INC.**
Erlanger, KY 41018 (US)

(72) Inventors:
- **Liang, Louis H.**
  Los Altos, California 94022-7420 (US)
- **Marinello, Daniel A.**
  Burlington, Kentucky 41005 (US)
- **Ryan, William J.**
  Underhill, Vermont 05489 (US)
- **Wray, Donald L.**
  Sunrise, Florida 33323 (US)

(74) Representative:
Luckhurst, Anthony Henry William
MARKS & CLERK,
57-60 Lincoln's Inn Fields
London WC2A 3LS (GB)

(54) Authentication system and method

(57) To authenticate and discriminate among articles, authentic articles are marked with predetermined concentrations of fluorescent substances having known emission wavelengths. The articles are illuminated, predetermined wavelength portions of the emission wavelengths are selected and measured, and then compared to previously characterised responses with respect to variables selected from the list consisting of

i) emission wavelengths,
ii) emission amplitudes,
iii) emission delay times, and
iv) spatial distribution.

A positive authentication result is produced if and only if the measured characteristics agree with the characterised responses.

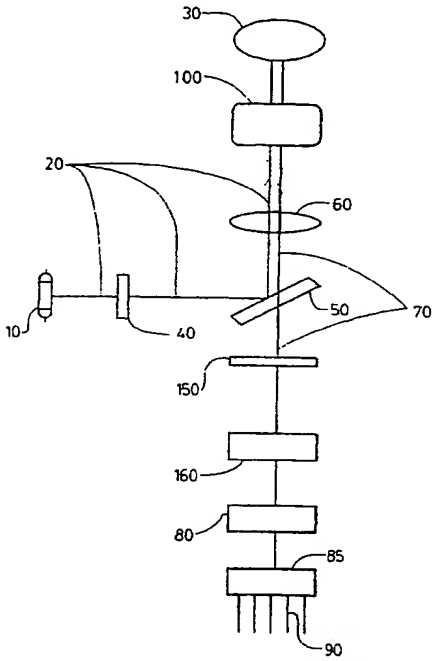

FIG. 1.

EP 1 178 429 A3

Printed by Jouve, 75001 PARIS (FR)

OCID: <EP___1178429A3_I_>

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 20 2851

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
D,A	US 4 642 526 A (HOPKINS F KENNETH) 10 February 1987 (1987-02-10) * the whole document * ---	1-3,5, 7-10,14, 17	G06K7/12 G06K19/10 G06K19/14 H04L9/00
A	FR 2 660 462 A (IXEA) 4 October 1991 (1991-10-04) * page 7, line 5 - page 8, line 24; figure 1 * ---	1,2, 17-20	
X Y	EP 0 268 450 A (LIGHT SIGNATURES INC) 25 May 1988 (1988-05-25) * page 3, line 7 - line 31; figure 1 * ---	24,26 25,27,28	
A	US 4 025 759 A (SCHEFFEL KURT M) 24 May 1977 (1977-05-24) * the whole document * ---	24-28	
Y	US 4 014 602 A (RUELL HARTWIG) 29 March 1977 (1977-03-29) * column 2, line 24 - column 4, line 45; figures 1-4 * * column 6, line 47 - column 7, line 2; figure 4 * ---	25,27	
Y	EP 0 488 177 A (MATSUSHITA ELECTRIC IND CO LTD) 3 June 1992 (1992-06-03) * claim 1 * ---	28	
A	US 4 127 773 A (WEST MICHAEL A) 28 November 1978 (1978-11-28) * column 4, line 8 - column 8, line 32; figures 1-9 * ---	29-31	
X A	US 5 005 873 A (WEST MICHAEL A) 9 April 1991 (1991-04-09) * column 6, line 1 - line 49; figure 8 * -----	32 29-31	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
G06K B07C

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	12 July 2002	Degraeve, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 20 2851

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

12-07-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4642526 A	10-02-1987	NONE	
FR 2660462 A	04-10-1991	FR 2660462 A1	04-10-1991
EP 0268450 A	25-05-1988	EP 0268450 A2	25-05-1988
		JP 63137386 A	09-06-1988
US 4025759 A	24-05-1977	NONE	
US 4014602 A	29-03-1977	DE 2501604 A1	22-07-1976
		AT 358299 B	25-08-1980
		AT 989875 A	15-01-1980
		BE 837634 A1	14-05-1976
		CH 613161 A5	14-09-1979
		DK 15476 A	17-07-1976
		ES 444319 A1	01-10-1977
		ES 458295 A1	16-06-1978
		FR 2298150 A1	13-08-1976
		GB 1541917 A	14-03-1979
		GB 1541918 A	14-03-1979
		IT 1054940 B	30-11-1981
		JP 51097333 A	26-08-1976
		LU 74184 A1	31-12-1976
		NL 7515010 A	20-07-1976
		SE 7600390 A	19-07-1976
EP 0488177 A	03-06-1992	EP 0488177 A2	03-06-1992
		JP 5197835 A	06-08-1993
US 4127773 A	28-11-1978	NONE	
US 5005873 A	09-04-1991	GB 2189800 A	04-11-1987
		AT 98570 T	15-01-1994
		DE 3788503 D1	27-01-1994
		DE 3788503 T2	14-04-1994
		EP 0267215 A1	18-05-1988
		WO 8706197 A1	22-10-1987

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82